Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-13. (Cancelled)

14. (New) A method of performing a cryptographic protocol between a first electronic entity and a second electronic entity in order to resist to an attack against the second electronic entity, comprising the steps of:

applying a message to both first and second electronic entities,

applying a first chain of operations to the message within the first electronic entity, so as to obtain a result,

determining a second chain of operations derived from the first chain of operations and applying the second chain of operations to the message within the second electronic entity so as to obtain a resultant message,

the step of determining the second chain of operations comprising

randomly selecting, for at least a part of the operations of the first chain of operations, to perform either the at least a part of the operations of the first chain of operations or the at least a part of the first chain of operations in a complemented state,

outputting as the resultant message, responsive to the step of randomly selecting, one of either a last operation of the first chain of operations, or a complemented result of the second chain of operations,

comparing the resultant message to the result.

15. (New) The method of claim 14, wherein the at least a part of the first chain of operations which can be performed in a complemented state comprises an exclusive OR.

16. (New) The method of claim 14, wherein the at least a part of the first chain of operations which can be performed in a complemented state comprises an operation of permutation of the bits of said message or of an intermediate result obtained on carrying out said second chain of operations until the operation of permutation of the bits of said message.

17. (New) The method of claim 14, wherein the at least a part of the first chain of operations which can be performed in a complemented state comprises an operation of indexed access to a table.

18. (New) The method of claim 14, wherein the at least a part of the first chain of operations which can be performed in a complemented state comprises an operation which

is stable with respect to the application of an exclusive OR function.

19. (New) The method of claim 18, wherein the at least a part of the first chain of operations which can be performed in a complemented state is an operation of transfer of the message or of an intermediate result obtained by carrying out said second chain of operations until the operation of transfer of the message, from one location to another one in a storage space.

20. (New) The method of claim 14, wherein the step of randomly selecting to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state comprises randomly selecting, for each of a series of several parts of the first chain of operations, to perform either such part in normal state or in complemented state.

21. (New) The method of claim 20, wherein the step of randomly selecting to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state comprises randomly selecting, for each of a series of operations of the first chain of operations, adjacent or not, to perform either such operation in normal state or in complemented state.

22. (New) The method of claim 20, wherein the step of randomly selecting to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in complemented state is conducted depending on the state of a random parameter generated for the at least a part of the first chain of operations and comprises updating a complementation counter, and the step of outputting as the resultant message is decided depending on the state of the complementation counter.

23. (New) The method of claim 20, wherein the step of randomly selecting to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state is conducted depending on the state of a random parameter generated for the at least a part of the first chain of operations and comprises transmitting, for each operation of the at least part of the chain of operations, information for deciding the step of outputting the resultant message.

24. (New) The method of claim 20, wherein the step of randomly determining and applying the similar chain of operations comprises the computing of a parameter which is equal to a difference between the number of times when an

operation of the first chain of operations was performed and the number of times when another one of the first chain of operations of the chain was performed in complemented state, and when this difference exceeds a given threshold, the decision to perform a next one of the second chain of operations in a complemented state is taken so as to decrease this difference.

25. (New) The method of claim 14, wherein the step of randomly determining the second chain of operations comprises selecting randomly to perform either the whole of the first chain of operations or all of the chain in complemented state selectively followed by a final complementing step.

26. (New) The method of claim 25, wherein the step of randomly selecting and applying the second chain of operations comprises computing a parameter which is the difference between the number of times when the operations of the first chain of operations were performed in normal state and the number of times when such operations of the first chain of operations were performed in a complemented state, and when this difference exceeds a given threshold, the decision to perform a next one of the second chain of

operations in a complemented state is taken so as to decrease this difference.

27. (New) The method of claim 14, wherein the complemented state of the at least a part of the first chain of operations is obtained by a complementation carried out byte by byte.

28. (New) The method of claim 14, wherein the complemented state of the at least a part of the first chain of operations is obtained by a complementation carried out bit by bit.

29. (New) The method of claim 14, wherein the step of determining the second chain of operations further comprises a step of determining a permutation of the order of successive commutative operations in the first chain of operations.

30. (New) The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. (New) The method of claim 21, wherein the step of randomly selecting to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state is conducted

depending on the state of a random parameter generated for the at least a part of the first chain of operations and comprises updating a complementation counter, and outputting as the resultant message is decided depending on the state of the complementation counter.

32. (New) The method of claim 20, wherein the step of randomly selecting to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in complemented state is conducted depending on the state of a random parameter generated for the at least a part of the first chain of operations and comprises transmitting, for each operation of the at least part of the chain of operations, information for deciding the step of outputting the resultant message.

33. (New) The method of claim 20, wherein the step of randomly determining and applying the similar chain of operations comprises the computing of a parameter which is equal to a difference between the number of times when an operation of the first chain of operations was performed and the number of times when another one of the first chain of operations of the chain was performed in complemented state, and when this difference exceeds a given threshold, the decision to perform a next operation of the second chain of

operations in a complemented state is taken so as to decrease this difference.